September 9, 2018

Via FCC Electronic Comment Filing System

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street SW, Room TW-A325
Washington, DC 20554

Re: Delivery of WEA to Subscriber Handsets (FCC-18-94, Docket 15-91 & 15-94)

Dear Marlene H. Dortch:
I would like to comment on Notice of Proposed Rulemaking (FCC-18-94) regarding the proposed "Preventing False Emergency Alerts and Improving Alert Testing" on the section about "Delivery of WEA to Subscriber Handsets."

If you have any questions concerning these comments, please do not hesitate to call (703-892-1810) or email (sean@donelan.com) me.

Respectfully submitted,

Sean Donelan

1. Errata and Technical Corrections

A reminder, the Commission has not corrected printing and technical errors in Part 11 accidently introduced while publishing past rulemakings:

> § 11.31(c) Since 2012, the second repetition of the example EAS header contains a lowercase "p" between "TTTT" and "JJJHHMM" instead of a hyphen "-". All three repetitions of the EAS header should be identical.
>
> § 11.31(f) Since 2003, the table of State, Territory and Offshore ANSI number codes (SS) repeats ANSI number "68" (Republic of the Marshall Islands - MH) and omits ANSI number "69" (Commonwealth of the Northern Mariana Islands - MP). Then the duplicate code "68" was removed, thus the Commonwealth of the Northern Mariana Islands – MP has been omitted from the table entirely. The table should include each State, Territory and District of Columbia code along with the National Weather Service marine areas once, and only once. Or incorporate by reference the ANSI, Census and National Weather Service geographic code definitions.

2. Delivery of WEA to Subscriber Handsets

As the FCC rules for Wireless Emergency Alerts (formerly CMAS) require handsets to implement more complex processing decisions and software programming, it will be impossible for an ordinary subscriber or carriers to divine what happened without data logs. Wireless handsets may or may not render an alert due to many reasons:

- Not in range of a carrier's infrastructure or roaming on partner's infrastructure without WEA
- WEA received, but specified geographic alerting polygon not including the current location
- The handset's estimate of its location, using differing geolocation technologies, may not be precise
- Subscriber choice to enable or disable alerts and buzzers
- Device not pre-empting an in-progress voice call or other user activity
- Should "cancelled" messages be rendered or hidden
- And probably other reasons

Even if the mobile device renders a WEA message, subscribers may miss hearing or seeing it immediately. Subscriber self-reporting about WEA performance is useful as a general survey, but corroborating data logs would be helpful. Android, iOS and likely other handset operating systems collect performance data about other aspects of the phone's performance as well as many Apps installed on the phone. However, consumer smart phones usually hide, don't collect or never report WEA performance data.

From a user interface design perspective, hiding obscure debug data makes sense because most consumers have little use for the information under ordinary circumstances. Worse, the confusing WEA logs may prompt calls to carrier customer service centers from questions with questions about the debugging data. On the other hand, during abnormal circumstances, such

as the Hawaii false alert, handset WEA performance data would be very valuable to determine what happened. Eyewitness recall can be confusing because different Apps may render non-WEA warning messages, or the user may not recall receiving a WEA message which was received.

FCC and FEMA should also avoid allegations of "tracking" phones through WEA data logs. Android and iOS report some operating system performance data and crash dumps to the OS developer, carrier or App developer. Because WEA is part of the handset base operating system, instead of an add-on third-party App, the performance data logs are likely part of the base OS logging collected by the Android, iOS or other operating system developer. FEMA, FCC or other government regulators in other countries which have similar mobile alerting systems would need to negotiate access to anonymized or non-personally identifiable aggregated WEA performance data collected from handsets.

Handset developers and carriers could be encouraged to create a user-friendly WEA history screen for consumers. Perhaps in an obscure part of the Settings menu consumers could check what happened to WEA messages during abnormal circumstances, but not too obvious that it causes excess customer care calls during normal circumstances. A WEA history screen could show when, where, and how WEA messages were received; and then why the handset alerted or did not alert. Obviously, a handset can't detect WEA messages sent while it was out of signal range.

FEMA and FCC should also encourage mobile operating system developers improve the WEA user interface to clearly distinguish between government issued WEA messages and alerts from other Apps on the phone. Advertisers and disruptive parties sometimes make their messages look like official alerts, such as the Postmates advertisement sent in Los Angeles (Figure 1 - Postmates Mobile Phone Advertisement April, 26, 2018). While the FCC can't prevent all messages, which look like fake alerts, handset developers could ensure only official WEA government alerts are stored on the WEA history page and uniquely rendered on other notification screens.

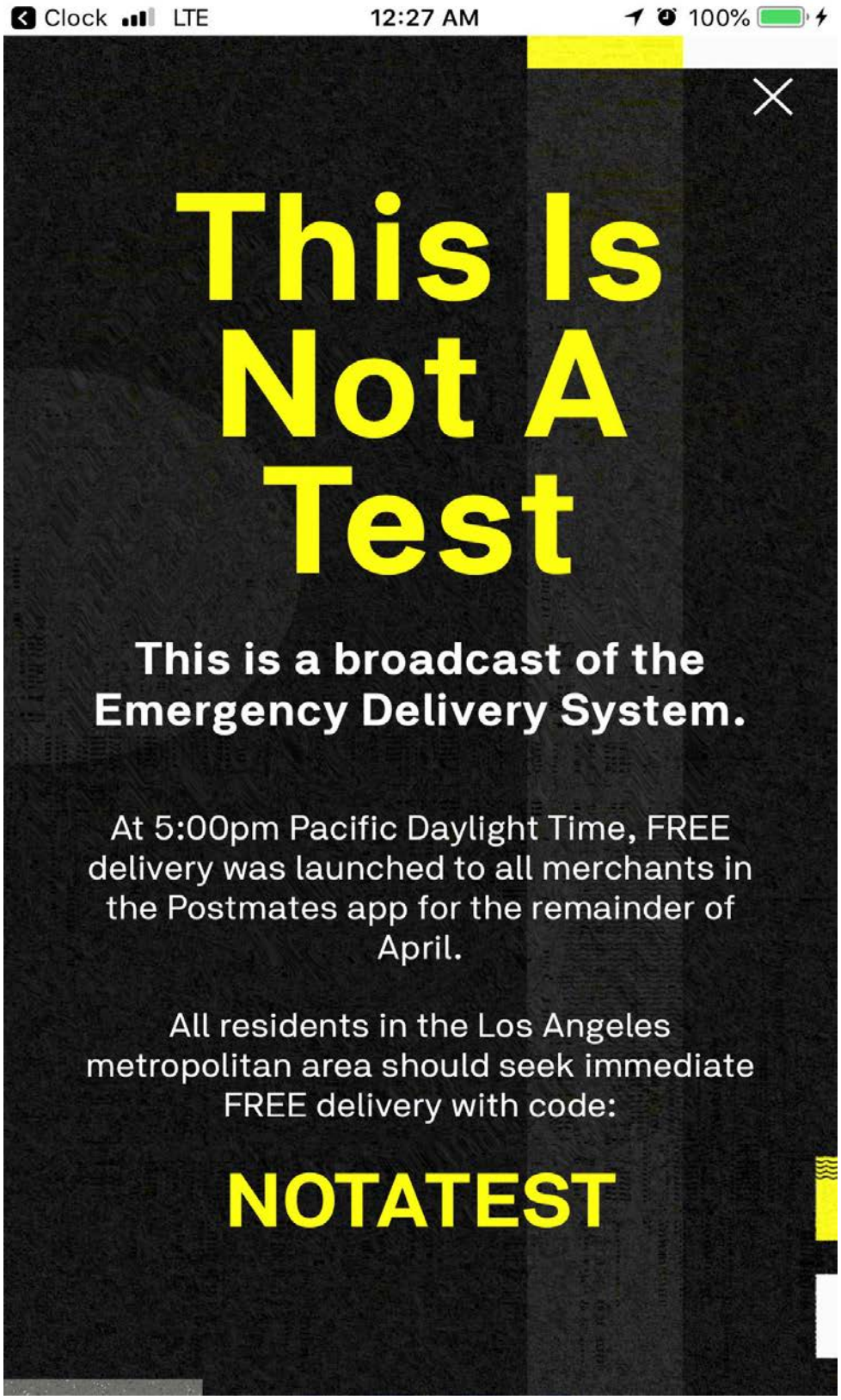

Figure 1 - Postmates Mobile Phone Advertisement April, 26, 2018